SOBERANÍA, RESISTENCIA Y AUTODEFENSA ELECTRÓNICA EN TELÉFONOS MÓVILES: PARTE 2

TU DISPOSITIVO. TUS DATOS. TUS REGLAS.

LA TECNOLOGÍA ES NUESTRA HERRAMIENTA, NO NUESTRA CADENA.

EN ESTE DOCUMENTO (ALGUNOS TEMAS):

ALTERNATIVAS A MOTORES DE BÚSQUEDA

Privacidad y neutralidad frente al monopolio de Google.

NAVEGADORES Y COMUNICACIONES PRIVADAS

Herramientas para navegar y comunicarte sin ser rastreado.

MENSAJERÍA SEGURA

Apps cifradas de extremo a extremo para proteger tus conversaciones.

CIFRADO Y HERRAMIENTAS DE PRIVACIDAD

Cifra tus datos, protege tus archivos y tu identidad digital.

SISTEMAS OPERATIVOS LIBRES PARA MÓVILES

Recupera el control de tu dispositivo con Android libre y sin Google.

REDES DESCENTRALIZADAS Y AUTONOMÍA

Tecnologías P2P, malla y autoalojadas para comunicar sin depender.

"La criptografía es la pólvora de la libertad en la era digital."

– Eric Hughes, Manifiesto Cypherpunk

Alternativas a motores de búsqueda

En lugar de depender del gran conglomerado de Google, hay motores de búsqueda diseñados para la privacidad y el control del usuario. Estas alternativas protegen la información de búsqueda y rompen el monopolio de datos:

- **DuckDuckGo:** Motor de búsqueda centrado en no rastrear al usuario. No almacena historiales de búsqueda ni perfiles de usuario y bloquea rastreadores de terceros. Su neutralidad de resultados reduce la influencia algorítmica. Para usarlo en Android, basta con instalar la app oficial o configurar el navegador predeterminado con DuckDuckGo como buscador, garantizando así búsquedas sin seguimiento. Este enfoque mitiga la amenaza de las burbujas de filtro y la construcción de perfiles comerciales basada en consultas.
- **StartPage:** Enfocado en anonimizar las búsquedas, actúa como intermediario entre el usuario y Google Search. Envía consultas a Google sin revelar la identidad del usuario ni la IP original. De este modo, resulta una forma de usar la base de datos de Google sin ceder datos personales. Se instala usando la app o añadiendo el buscador a la configuración de navegadores; bloquea al mismo tiempo cookies de seguimiento. Así combate la vigilancia masiva de Google al separar la persona física de la consulta.
- **Qwant:** Motor europeo que promete neutralidad informativa y privacidad. No usa cookies de seguimiento ni perfiles de usuario. Ofrece resultados basados en fuente abierta y filtros personalizables. Su enfoque desde la Unión Europea lo posiciona como escudo contra la extracción de datos estadounidense. Se configura fácilmente agregándolo como buscador predeterminado en el navegador Android y deshabilitando el uso de la cuenta Google. Mitiga la centralización global de datos de búsqueda y protege contra la minería comercial de hábitos.
- **MetaGer:** Servicio europeo que combina varias fuentes de búsqueda con énfasis en anonimato. Actúa como meta-buscador: envía consultas a otros motores detrás del usuario. Ofrece opciones de cifrado de la petición. Integrarlo en el teléfono móvil puede lograrse mediante el navegador o su app, configurando las preferencias para no rastrear. Sirve de barrera contra la recopilación de clics individuales, lo que dificulta la vigilancia de consultas específicas por parte de entidades comerciales o de inteligencia.
- **Kagi:** Motor de búsqueda privado más reciente, centrado en un modelo de suscripción sin anuncios. No recoge datos de usuario ni personaliza los

resultados según historiales. Su diseño minimalista favorece respuestas directas. Es una resistencia al modelo publicitario: reemplaza ingresos por anuncios con cuotas voluntarias. La instalación y uso es vía web/app oficial. Al no depender de publicidad ni perfiles, neutraliza la monetización de la actividad de búsqueda.

- **Brave Search:** Alternativa de privacidad emergente, parte del ecosistema Brave. Utiliza un índice propio y no rastrea al usuario ni vende datos. Se integra en el navegador Brave, permitiendo búsquedas privadas integradas. Evita el rastreo porque no asocia consultas a cuentas. Bloquea scripts invasivos típicos de motores corporativos. Su uso en Android es natural si se emplea el navegador Brave: de este modo, las búsquedas no alimentan perfiles comerciales, reforzando la independencia informativa.
- **Mojeek:** Motor británico que tiene su propio índice independiente. Reconocido por no espiar a los usuarios. Su algoritmo devuelve resultados sin seguimiento histórico. Se puede usar agregando el sitio como buscador o mediante la app disponible. Mojeek evita entregar información a terceros, mitigando la amenaza de alianzas de datos corporativos que explotan las consultas individuales.
- **Ecosia:** Motor de búsqueda que destina ganancias a plantación de árboles. Aunque usa índices de terceros (Bing), promete no vender datos ni crear perfiles. Al usarlo, en la práctica el usuario tiene búsquedas privadas y contribuye a causas sociales. Se instala como buscador en Android fácilmente. Resiste la extracción de datos al desvincular los ingresos directos de la publicidad, reduciendo así incentivos corporativos de explotación de la información de búsqueda.
- **Whoogle:** Interfaz autohospedada tipo proxy de Google Search. Permite realizar búsquedas en Google sin que Google reciba datos de usuario. Técnicamente, se instala en el propio servidor o móvil como backend ligero. Configurándolo se usa Google Search sin ceder la IP real ni cookies. Neutraliza la vigilancia al actuar como cortafuegos entre Google y el usuario.
- **Yacy:** Red de búsquedas descentralizada. Cada usuario contribuye con su propio índice de búsqueda P2P. No hay servidor central; la privacidad es intrínseca al diseño. Instalando la aplicación Yacy en un dispositivo Linux (o compatible) y conectándolo a la red, el teléfono obtiene búsquedas colaborativas sin depender de corporaciones. Mitiga la amenaza de control central al dispersar la indexación, volviendo imposible para cualquier empresa monitorear todas las consultas.

- **Searx:** Metabuscador de código abierto que combina resultados de varias fuentes (Google, Bing, otros) sin rastrear usuarios. Los resultados se agregan en un solo lugar sin cookies. Se puede usar vía navegadores apuntando al servidor Searx público o instalar la propia instancia. Permite navegación privada, impidiendo que los grandes portales vean patrones de búsqueda. De esta forma, rompe la correlación de datos entre cuentas e intereses de búsqueda.
- **4get:** Buscador ligero diseñado para privacidad. Similar a Searx, usa diversos índices al tiempo que bloquea el rastreo. Se instala como app o se configura en el navegador. Filtra scripts invasivos y no almacena datos de búsqueda. Su uso combate la minería de datos porque ninguna consulta queda registrada bajo identidad alguna.

Alternativas a YouTube

El monopolio de Google en vídeo se contrarresta con aplicaciones que permiten ver contenidos multimedia sin dar información personal ni ser bombardeado por publicidad. Cada una es un acto de resistencia digital:

- **NewPipe:** Cliente Android libre para ver vídeos de YouTube y otras plataformas sin Google Play Services ni anuncios. Se descarga desde F-Droid o su página oficial. Permite reproducir vídeos en segundo plano, en ventana flotante, descargar medios y escuchar solo audio. Consume la API pública de Invidious (proxy de YouTube) de forma que Google no recibe datos de la visualización. Esto impide que YouTube construya perfiles de consumo de contenido o muestre sugerencias basadas en el historial. Para implementarlo, hay que instalar la APK actualizada y habilitar en ajustes su modo de fondo. Así, cada reproducción se realiza “de incógnito” respecto a Google.
- **PipePipe (NewPipe Enhanced):** Versión ampliada de NewPipe desarrollada por la comunidad. Agrega funciones extra como integración de cuentas (para contenidos restringidos), filtrado avanzado de búsqueda y bloqueos selectivos (por ejemplo, Skip sponsorblock para saltar anuncios internos). Se instala vía F-Droid. Conserva la privacidad de NewPipe pero ofrece más control al usuario. Implementarlo implica configuraciones adicionales en el menú: activar la opción de inicio de sesión externo si se desea ver vídeos de contenido restringido, personalizar categorías de filtro, etc. Este cliente mejorado complica aún más la vigilancia de Google ya que ni siquiera la interacción con vídeos “solo para adultos” se asigna a una cuenta de Google.

- **LibreTube:** Aplicación FOSS que utiliza “Piped”, otro proxy de YouTube. Bajo el capó usa contenedores independientes para cada usuario, e incluye complementos como SponsorBlock y ReturnYouTubeDislike. Se instala por F-Droid o APK, y permite crear instancia personal de Piped para mayor independencia. En términos de autodefensa, LibreTube protege la identidad del usuario porque toda la consulta y reproducción viaja en la propia infraestructura de Piped. Configurando LibreTube se activan extensiones de privacidad (por ejemplo, sombreado automático de thumbnails para privados) y se puede forzar HTTPS siempre. Así garantiza resistencia a la censura y vigilancia de Google.
- **FluxTube:** Aplicación multiplataforma basada en Flutter que admite múltiples backends (NewPipe-Extractor, Piped, Invidious, Explode). Su fortaleza es la redundancia: si Google bloquea un servicio Invidious, FluxTube puede cambiar de backend al vuelo. Se instala desde F-Droid/Play. Es ligera y ofrece modo oscuro, historial. Al ejecutar video, FluxTube elige el servidor de extracción de información, reduciendo la posibilidad de que Google bloquee una sola vía. Implica resistencia táctica: aun si un proxy falla, siempre hay otro que se puede usar. Para la configuración, se elige servidor preferido o se deja en modo automático. Las amenazas de cambio repentino en APIs de Google se neutralizan con este enfoque multi-servidor.
- **YouPipe:** Interfaz moderna de NewPipe con diseño Material3. Soporta suscripciones y reproducciones en segundo plano. Se instala en Android de manera convencional. Comparte la filosofía de privacidad: nada se envía a Google. La ventaja de YouPipe está en su accesibilidad UI; funciona igual que NewPipe en cuanto a privacidad, pero resulta más intuitiva para algunos usuarios. Para configurarlo, simplemente se añaden canales favoritos y se elige la aplicación de vídeo preferida (por ejemplo VLC) para reproducción. Su uso cotidiano facilita el alejamiento de la interfaz web de Google, al mismo tiempo que conserva la soberanía de datos.
- **LiTube:** Navegador especializado que carga YouTube en WebView limpio, bloqueando anuncios y trackers. Funciona como un navegador interno con opciones avanzadas: reproductor pop-up, lista de reproducción, descarga. Se instala por F-Droid. A pesar de depender del sitio web de YouTube, LiTube reduce la exposición del usuario: no manda la cookie de cuenta y su motor bloquea publicidad automáticamente. Configurarlo incluye otorgar permisos de descarga y elegir reproductor interno o externo. Aunque no es completamente descentralizado, ayuda a romper la rutina de abrir

YouTube directamente en el navegador principal, desviando el tráfico a un entorno controlado que no reporta datos de forma transparente a Google.

- **SkyTube:** Cliente FOSS que utiliza la librería NewPipe para obtener vídeos, con un fuerte enfoque en control de contenido. Permite filtrar vídeos no deseados, gestionar suscripciones, canales y listas de reproducción. Se instala fácilmente. Es completamente offline-friendly; puede buscar y reproducir vídeos sin guardar cookies. En el contexto de autodefensa, al estar basado en código abierto y no requerir servicios de Google, SkyTube ofrece un entorno de visualización desconectado. Configurarlo implica importar archivos OPML con suscripciones o ajustar parámetros de filtrado (por ejemplo, ocultar vídeos por palabra clave). Ayuda a neutralizar las recomendaciones algorítmicas invasivas y la sobreexposición publicitaria, cortando la transmisión de datos a los algoritmos de YouTube.
- **LearnTube:** Enfocado en aprendizaje, extiende NewPipe con seguimiento de progreso y notas. Se diseña para utilizar YouTube como recurso educativo sin elementos distractores. Protege la privacidad al igual que NewPipe (no requiere cuenta Google). Para la implementación, se pueden crear listas de vídeos de cursos y añadir notas. Esta herramienta empodera al usuario a educarse sin dar autoridad a Google: cada visualización queda aislada y no participa en métricas de consumo de contenido general. Funciona como una capa académica que respeta la intimidad.
- **WizeStream**: WizeStream es un cliente de streaming independiente para Android, basado en NewPipe y licenciado bajo GPLv3, diseñado para maximizar la privacidad y la soberanía digital. Elimina toda dependencia de servicios de Google, cuentas o rastreo, operando bajo un modelo "local-first" donde historial, suscripciones y listas se almacenan localmente. Su funcionalidad incluye reproducción en segundo plano, descargas, integración con SponsorBlock y soporte multiplataforma (YouTube, PeerTube, SoundCloud). Destaca técnicamente por su sincronización peer-to-peer cifrada entre dispositivos de confianza, eliminando servidores en la nube y preservando la integridad de los datos personales. Al ser de código abierto, sin telemetría y con actualizaciones firmadas verificables, empodera al usuario frente a ecosistemas propietarios, garantizando control absoluto sobre su consumo multimedia y metadatos, incluso en contextos de alto riesgo o activismo digital.
- **Flow**: Flow es un cliente de YouTube y YouTube Music para Android, licenciado bajo GPLv3, que prioriza la privacidad y la soberanía digital mediante su motor de recomendaciones "FlowNeuro". Este algoritmo opera 100% en el dispositivo, aprendiendo de los hábitos de visualización sin

enviar telemetría, requerir cuentas de Google ni depender de servidores externos. Garantiza la protección de datos al almacenar todo localmente, ofreciendo un panel de transparencia para inspeccionar, ajustar, exportar o eliminar el perfil de recomendaciones en cualquier momento. Compatible con importaciones desde NewPipe, fomenta la independencia del ecosistema propietario. Aunque depende de la red de YouTube (limitando su soberanía total), elimina anuncios, rastreo y análisis, empoderando al usuario con un descubrimiento de contenido personalizado, seguro y completamente autónomo, alineado con la resistencia digital y el control absoluto sobre su huella de datos personales.

Launchers de Android (Interfaces de inicio)

El launcher (pantalla de inicio) es la primera capa de la experiencia móvil. Sustituir el launcher de Google por uno libre fortalece la soberanía: elimina rastros de datos persistentes y reduce el control corporativo del dispositivo. Estos lanzadores alternativos enfatizan simplicidad y privacidad:

- **Pie Launcher:** Interfaz radical basada en gestos: deslizar desde cualquier borde muestra un menú circular (la “tarta”) con accesos a aplicaciones frecuentes. Oculta el grid tradicional, optimizando el uso a través de la memoria muscular. Instalándolo y asignándolo como predeterminado, se reemplaza la pantalla principal convencional. No requiere permisos especiales y no se comunica con servidores externos, lo que significa que todo el diseño e historial de uso queda local. El modelo de gestos anonimiza la interacción, ya que no hay almacenamiento de preferencias en la nube.
- **Last Launcher:** Lanzador minimalista de una sola página con lista de aplicaciones. Eliminando iconos, usa solo texto con fuentes personalizables y colores. Su simplicidad extrema asegura bajo consumo energético y uso de RAM. Al usar Last Launcher, se elimina cualquier elemento de rastreo o anuncio; no contiene permisos de red. La configuración incluye elegir orden de las apps y tema de color. La pantalla es tan básica que prescinde incluso del feed de Google o widgets intrusivos. Esto neutraliza la amenaza de interfaces adictivas: el usuario ve solo el contenido esencial, dificultando el seguimiento visual del comportamiento.
- **DroidOS Launcher:** Parte de una suite avanzada para productividad. Incorpora un “launcher flotante” en forma de burbuja interactiva que abre un gestor de ventanas con mosaicos (tile layout) estilo sistema de ventanas. Requiere habilitar permisos especiales (accesibilidad) y opciones de desarrollador (ventanas libres). Al instalarlo, se desactiva en gran medida

la interfaz estándar de Android; en su lugar, se lanza la burbuja y se colocan ventanas de apps en mosaico. Esto aumenta la soberanía, pues permite multitarea real y esquiva el launcher impuesto por el fabricante. A nivel de amenazas, recupera el control de las ventanas: apps flotantes no notifican a Google que han sido abiertas, y el uso simultáneo complica la monitorización de actividad por app. Para configurarlo, se siguen los pasos del proyecto: instalar APKs, dar permisos a Shizuku (similar a root), y configurar accesibilidad. Esto otorga un entorno de trabajo mucho más libre, escapando de la rigidez de la interfaz de Google.

- **Dragon Launcher:** Diseñado para ser operativo mediante gestos, con barra de estado personalizable y enfocado en la eficiencia. Permite lanzar apps con deslizamientos rápidos y oculta la barra de notificaciones si se desea. No posee permisos extraños ni conexión a internet: es totalmente offline. Durante la instalación, se debe desactivar la protección de Play (para evitar bloqueos) y concederle accesibilidad para funciones adicionales (por ejemplo, bloquear pantalla o manejar notificaciones). Al hacerlo, el usuario obtiene un lanzador que prioriza la privacidad: Dragon no recopila ni envía datos. Su uso combate la intrusión al no recolectar estadísticas de uso. Se configura asignando gestos, colores y widgets, manteniendo un perfil tecnológico independiente de Google.
- **Ion Launcher:** Equilibra estética y productividad. Organiza automáticamente el cajón de apps por categorías, mostrando sólo las apps relevantes en el home. Permite widgets y configuraciones de color. Si bien solicita algunos permisos (reloj, almacenamiento), no envía datos a terceros. Instalándolo y asignándolo, ofrece un estilo de navegación diferente al de Google. Su valor para la soberanía radica en el aislamiento del ecosistema: al categorizar offline, la información de qué apps usa se mantiene en el dispositivo y no alimenta algoritmos externos. Se puede personalizar fondo, tema oscuro, búsqueda integrada, todo sin ads ni seguimiento.
- **Olauncher:** Extremadamente minimalista: un solo panel de aplicaciones con reloj grande. No muestra iconos ni nada llamativo; reduce el tiempo de pantalla bloqueando distracciones. Para instalador se encuentra en tiendas alternativas. Su ventaja es forzar una rutina casi “dumbphone”: solo lo esencial visible. Elimina cualquier seguimiento porque no hay búsquedas incorporadas ni conexiones a internet. Al activarlo, el uso del dispositivo se vuelve deliberado: cada abrir de app es consciente, sin sugerencias o publicidad de inicio. Como autodefensa, reprime la adicción al

smartphone. Se configura poco: básicamente con activar o desactivar el fondo animado, nada más.

- **FokusLauncher:** Otro lanzador de texto puro, similar a Last Launcher. Solo presenta nombres de apps (sin iconos) en fuentes uniformes. Reduce distracciones visuales y acelera el acceso por búsqueda de texto. Al usarlo, el sistema deja de generar imágenes o interfaces avanzadas; todo es texto. No conecta a nada y apenas pide permisos. La resistencia tecnológica se manifiesta en su simplicidad: nada de tracking gráfico ni personalización profunda, lo que priva a cualquiera de información personal más allá de las consultas de app.
- **Murine Launcher:** Minimalista con predilección por la velocidad. Muestra apps en lista alfabética y permite filtros rápidos. Diseño austero, muy bajo consumo. No recolecta datos y es completamente offline. Al usarlo, el usuario elimina cualquier uso de servicios externos como Google Feed o Pocket, pues todo se maneja localmente. Configurar Murine es básico: organizar orden de apps según preferencia. Con este launcher se refuerza la soberanía al mantener el control en la configuración local de la pantalla.
- **Neat Launcher:** NeatLauncher es un lanzador de Android minimalista y de código abierto que sustituye la interfaz tradicional de iconos y widgets por una lista de texto limpia, priorizando la velocidad y la eficiencia operativa. Su funcionamiento se articula en torno a un motor de búsqueda unificado que permite localizar y ejecutar aplicaciones, contactos o consultas web desde un único punto, gestionado mediante gestos personalizables y la capacidad de renombrar, reordenar u ocultar elementos de la vista principal sin que estos pierdan su indexación global. Este modo de uso, desprovisto de telemetría y funciones pesadas, ofrece una interacción fluida, segura y directa con el dispositivo, resultando ideal para quienes buscan un control absoluto y una experiencia digital libre de distracciones a través de atajos inteligentes y comandos de texto.
- **Yagni Launcher:** Aunque todavía en desarrollo, adopta el principio “You Aren’t Gonna Need It”: interfaz personalizable hasta el extremo (puede cambiar todos los elementos de la cuadrícula, color, iconos). Aún en fase Alpha, promete ser pequeño (2 MB) y sin rastreadores. Instalándolo desde F-Droid, reemplaza el launcher estándar con uno ultraligero. Al suprimir funcionalidades innecesarias (evitando bloatware), reduce vectores de seguimiento, pues cada cambio queda local y controlado. Su estrategia de diseño implica que el usuario no tiene que ceder datos a servidores para personalizarlo; todo se ajusta internamente. Se configura ajustando tamaño de grilla y estilo, sin perder control sobre su privacidad.

- **YAM Launcher:** “Yet Another Minimalist”, pantalla inicial basada en texto con integración opcional de clima. Muestra fecha, temperatura y accesos directos. Se instala desde tienda o repositorio. No utiliza internet si no se le indica (por ejemplo, la info del tiempo es de Open-Meteo). Con YAM, el teléfono se convierte en un dispositivo centrado en el aquí y ahora, con menos distracción de apps, ya que encabeza la pantalla con información esencial. Este launcher organiza brevemente el entorno sin vender datos al colocarlo como predeterminado; la descarga opcional de la capa del tiempo es la única interacción de red, que se podría desactivar para máxima autonomía. Así se rechaza el entorno visual de Google y se privilegia la vida offline.

Alternativas a Google Calendar (Calendarios y Tareas)

La gestión de la agenda y tareas mediante Google implica una vigilancia constante del cuándo y dónde. Estas herramientas reemplazan el calendario corporativo por soluciones cifradas o locales:

- **Proton Calendar:** Parte del ecosistema Proton (mismo servicio suizo de email). Ofrece calendario cifrado de extremo a extremo. Cada evento (título, descripción, participantes) se almacena cifrado en servidores en Suiza sin claves de acceso por terceros. Se instala la app oficial de Proton en Android y se activa la sincronización de Calendar. El usuario tiene control total de permisos, y la información nunca se envía en texto plano. Esto neutraliza la amenaza de espionaje corporativo: eventos personales no nutren bases de datos públicas ni algoritmos comerciales.
- **Tuta Calendar:** De la plataforma Tutanota. Similar a Proton, todo se cifra localmente. Además incluye cifrado pos-cuántico en metadatos. La aplicación se obtiene de la tienda de Tuta o repositorios seguros. Luego se configura dentro de la app de calendario de Tutanota. Al usarlo, cada reunión o recordatorio queda protegido incluso ante futuros supercomputadores cuánticos. La soberanía tecnológica aquí es absoluta: el calendario y los correos asociados solo los descifta el propietario, impidiendo que servicios de inteligencia (o Google) lean el contenido de eventos.
- **EteSync:** Plataforma independiente para sincronizar contactorios, calendarios y tareas con cifrado de extremo a extremo. Se crea una cuenta EteSync e instala su app junto con el complemento *DAVx⁵* para Android. Al crear un nuevo calendario en EteSync, este se importa en las apps estándar de calendario (p. ej. AOSP Calendar). La información sincronizada (eventos,

contactos) viaja cifrada con contraseña local. Así ningún servidor, ni siquiera de EteSync, puede acceder a los datos en claridad. Frente a Google, esto aísla completamente el contenido: incluso si se interviene el servidor, los datos no se leen.

- **kSync:** Aplicación (de Infomaniak) diseñada para sincronizar calendarios CalDAV fácilmente en Android. Aunque apunta a usuarios de Infomaniak, funciona con cualquier servidor compatible. Permite ver Google Calendar mediante CalDAV como puente, reduciendo dependencia de las APIs internas de Google. Al usar kSync (configurando credenciales CalDAV del servidor deseado), se evita exponer la cuenta Google a apps de terceros. Es una capa de abstracción que fortalece la privacidad de horarios al utilizar protocolos abiertos. Implementarla implica permitir la aplicación para acceder a Contactos/Calendarios en Android, pero luego todos los eventos se gestionan fuera del ecosistema Google.
- **Cfait:** Gestor de tareas offline y basado en texto. Se integra con el teléfono como app independiente para listas de tareas (To-Do). Al guardar tareas localmente (o sincronizar con servicios compatibles vía DAVx), no hay servidor externo ni cuenta necesaria. Instalar Cfait (disponible como APK en F-Droid) y organizar listas con etiquetas o fechas ofrece protección ante Google Tasks. Como no requiere internet, la amenaza de que Google analice o reclame datos de pendientes desaparece. Es útil para tareas rápidas sin exposición: incluso la creación de una lista de compras queda en el dispositivo.
- **DAVx⁵:** Esencial para calendarios/tareas en Android. Este cliente permite conectar calendarios CalDAV, contactos CardDAV y tareas VTODO a cualquier servidor libre (Nextcloud, Baïkal, etc). Al instalarlo y configurar una cuenta CalDAV (por ejemplo, con Proton o Tuta), DAVx⁵ sincroniza eventos en la app de calendario estándar del móvil. Actúa de mediador cifrado opcional, lo que elimina la necesidad de apps de Google para sincronizar datos. Así, la agenda del usuario se aloja donde él elija, rompiendo el monopolio de sincronización que Google tiene por defecto. El uso de DAVx⁵ convierte cualquier servidor propio en tu Google Calendar privado.
- **Tasks (Tasks.org):** Gestor de tareas heredero de Astrid. Administra listas de tareas locales o sincronizadas por CalDAV/EteSync. Se instala en Android (F-Droid). Se puede usar completamente offline o enlazarlo con DAVx⁵/EteSync para sincronización cifrada. Esto rompe la dependencia de Google Tasks. Usándolo, el registro de pendientes queda bien organizado sin filtrado. Es ideal para autodefensa cotidiana: desde la simple lista

“hacer ejercicio” hasta la planificación de proyectos, todo resguardado de la vigilancia porque no se almacena en la nube de Google.

- **JtxBoard:** Aplicación Android (menos conocida) enfocada en tareas y diarios en formato caldav. Suele usarse con Nextcloud News/Tasks para manejar VTODO/NOTE. Instalarla y conectarla vía DAVx[5] a un servidor Nextcloud añade una interfaz de calendario/tareas centralizada. En este ecosistema, Google pierde control: el calendario de tareas se gestiona en servidores autohospedados. Cada nota o tarea se guarda en tu propio sistema, evitando la concentración de metadatos que Google generaría con cada recordatorio.
- **OpenTasks:** Aplicación vieja pero funcional para listas de tareas. Descarga desde F-Droid e instala junto con DAVx[5] para sincronizar con servidores CalDAV compatibles. Permite crear tareas con alertas, categorías y recorridos. Al funcionar offline también, el historial de tareas nunca llega a Google. Cada tarea se mantiene en el dispositivo o en el servidor elegido (por ejemplo, Nextcloud), asegurando que las actividades planeadas permanezcan privadas.
- **KashCal:** Calendario unificado que agrega varios servicios (Google, iCloud, CalDAV, etc) en una sola vista. Aunque su uso principal es visualizar calendarios de distintas cuentas, su contribución a la soberanía está en permitir migrar o conectarse a servicios descentralizados (p. ej. mostrar Proton y Nextcloud juntos). Para implementarlo, se configuran las diferentes cuentas de calendario. KashCal actúa como una placa unificadora, facilitando el uso de soluciones privadas junto con externas. A nivel de resistencia, da flexibilidad: el usuario puede integrar calendarios cifrados (Proton, EteSync) en la misma app, reduciendo la tentación de volver a Google Calendar para “ver todo en un lugar”.

Alternativas a Gmail (Correo)

Reemplazar la cuenta de Gmail es esencial para romper la dependencia del ecosistema de Google. Las opciones disponibles ofrecen cifrado, filosofía de servicio libre y soberanía jurisdiccional:

- **ProtonMail:** Servicio suizo de correo cifrado de extremo a extremo. Ofrece apps móviles seguras donde los mensajes se cifran en el dispositivo antes de subirlos al servidor. La interfaz (web o app de Android) es intuitiva y no almacena tus claves. Para implementar, se instala la app oficial y se crea una cuenta. Todas las transmisiones van cifradas, impidiendo que cualquier intermedio (incluido Proton) lea el contenido. Al reemplazar

Gmail con ProtonMail, el usuario pone sus emails bajo protección legal suiza y tecnológica. Resiste la vigilancia masiva porque ni Google ni terceros pueden espiar las comunicaciones cifradas.

- **StartMail:** Servicio de correo holandés enfocado en la privacidad. No posee app dedicada en Android, pero usa protocolos estándares (IMAP/SMTP) que se configuran en cualquier cliente. Ofrece alias autodestruibles y no escanea correos para publicidad. La implementación consiste en registrar cuenta y conectarla con una app como FairEmail. Al hacerlo, Gmail queda sustituido por un buzón que no escanea ni vende datos. Esto refuerza la soberanía al no alimentar a Google con metadatos de emails y al asegurar que los proveedores cumplan leyes europeas de privacidad en lugar de las propias de empresas estadounidenses.
- **AxiChat:** Aunque se menciona en Gmail, AxiChat es en realidad un cliente universal de correo (y chat) descentralizado. Permite agregar cuentas de email (incluso GMail) y protocolos XMPP/Matrix. Es FOSS y no asocia identidad. Instalar AxiChat implica configurar servidores IMAP/SMTP propios. Así, se libera al usuario del cliente propietario de Google. Cualquier correo gestionado aquí escapa del escrutinio de Google (su app no comparte datos de mensajería). Además, al soportar múltiples protocolos, fomenta ecosistemas federados (Matrix) como alternativa a los chats corporativos.
- **Tuta Mail (Tutanota):** Correo alemán gratuito con cifrado E2EE. Su app en Android cifra automáticamente asunto y cuerpo de emails. Para usarlo, se registra la cuenta Tutanota y se descarga la app Tuta. No usa estándares abiertos para el cifrado, pero ofrece confidencialidad total al usuario. Al sustituir a Gmail por Tutanota, se asegura que ni siquiera el proveedor puede leer los correos sin autorización explícita. Lo que se discute en tus emails queda blindado frente a vigilancia corporativa.
- **FairEmail:** No es proveedor, pero es un cliente de código abierto para Android. Permite conectar múltiples cuentas IMAP/SMTP (por ejemplo Proton, StartMail, mailbox.org). Resalta por su control de privacidad: usa encriptación PGP/GPG opcional para almacenar localmente, y no incluye código propietario ni trackers. Instalándolo, se configura con los parámetros de cualquier proveedor libre. Esto habilita usar cuentas alternativas con total transparencia. Al usar FairEmail en vez de la app Gmail, cada correo recibido o enviado pasa solo por protocolos estándares sin intervención de Google. Mitiga la amenaza de la app de Gmail que pudiera escanear o indexar correos.

- **kMail:** La aplicación kMail (Infomaniak Mail) para Android, disponible en F-Droid (sin notificaciones push) y bajo licencia GPL-3.0, es un cliente de código abierto en Kotlin que prioriza la soberanía digital y la nula telemetría. Su arquitectura usa la API de Infomaniak para evitar el bloqueo de IMAP en el extranjero y prevenir el scraping por terceros, garantizando disponibilidad global para activistas y profesionales. Protege los datos mediante cifrado interno transparente y externo con estándares OpenPGP, criptografía de curva elíptica (ECC) y AES-256-GCM, ocultando el contenido en búsquedas. Alojada en Suiza bajo FADP/GDPR, sin publicidad ni análisis de correos, ofrece autenticación robusta, bloqueo a nivel de dispositivo y defensa avanzada contra phishing, consolidándose como una alternativa técnica, segura y federada para la resistencia digital y el uso cotidiano .
- **mailbox.org:** Proveedor alemán de pago (con opción básica gratuita), parte de GNU social suite. Ofrece correo, calendario y nube. No utiliza datos de usuarios para publicidad. Se accede mediante cliente o web, y se puede configurar en FairEmail o K9. Los servidores en Alemania están sujetos a leyes estrictas de privacidad. Implementándolo, el usuario migra a un correo gobernado cooperativamente. Es un acto de autodefensa ya que los mensajes no alimentan los algoritmos estadounidenses y el contenido se guarda bajo jurisdicción comunitaria.
- **Cock.li:** Cock.li (www.cock.li) es un servicio de correo centrado en el anonimato que omite la recolección de datos personales, recomendando el uso de Tor o VPN. Aunque implementa cifrado en reposo, carece de cifrado de extremo a extremo (E2EE) nativo, autenticación en dos pasos (2FA) y protocolos de federación segura, transmitiendo mensajes sin encriptación si el servidor destino no soporta TLS. Su arquitectura retiene metadatos críticos (IP, user agent y logs IMAP/SMTP por 48-72h), escanea contenido antispam y cumple órdenes legales. Dado su historial de brechas con más de un millón de registros expuestos , resulta útil únicamente para identidades desechables o resistencia digital básica, siendo insuficiente para proteger datos sensibles sin cifrado externo (PGP) y una estricta higiene operativa.
- **Sterna Mail:** Sterna Mail es un cliente de correo nativo para Android, FOSS y disponible en F-Droid, diseñado para protocolos JMAP e IMAP/SMTP sin servicios de Google ni rastreo. Su arquitectura prioriza la privacidad mediante cifrado OpenPGP de extremo a extremo delegado a OpenKeychain, garantizando que las claves privadas nunca toquen su proceso y que el texto descifrado solo resida en memoria volátil (caché LRU), sin persistencia en disco. Implementa un enfoque "offline-first" con

caché Room, notificaciones push mediante UnifiedPush (evitando FCM) y endurecimiento de seguridad: verificación estricta de TLS, bloqueo por defecto de contenido remoto en WebView, prevención de inyección de cabeceras SMTP, protección contra capturas (FLAG_SECURE) y limpieza de parámetros de rastreo. Es una herramienta robusta y soberana para activistas y usuarios que exigen confidencialidad, cifrado y cero dependencia de ecosistemas propietarios.

- **Autistici/Inventati:** Servicio comunitario italiano provisto por voluntarios. Ofrece email, calendarios y web hosting. Gratuito y cifrado moderado. Para usarlo se crea cuenta y se conecta vía IMAP. Al migrar a A/I (nombre original en italiano), el usuario entra a una comunidad que rechaza fines comerciales. Los correos sólo viajan dentro de un sistema pequeño, lo cual es un acto de resistencia porque no financia plataformas masivas ni expone los datos a redes globales.
- **Disroot:** Servicio cooperativo holandés que incluye email cifrado. Con soporte para IMAP. Se accede mediante cliente propio o configurando en apps libres. Al usar Disroot, se entra a un ecosistema de servidores libres. Pone en manos del usuario final la soberanía sobre sus datos, pues la infraestructura es gestionada por activistas que no obedecen a intereses comerciales.
- **Riseup:** Conocido servicio de correo para activistas (EE. UU.). Aunque limitado (solo invitaciones), garantiza privacidad y cifrado. Su app es mínima, se puede configurar Riseup en cualquier cliente IMAP en Android. Migrar a Riseup implica confiar la correspondencia al proyecto comunitario, evitando a Google. Los emails pasan por su servidor, que está orientado a causas sociales, no a lucro, reduciendo la posibilidad de vigilancia corporativa de mensajes.

Alternativas a Google Drive (Almacenamiento en la nube)

Guardar archivos en la nube de Google implica que la información personal reside en infraestructura corporativa. Las siguientes opciones cifran o autohospedan el almacenamiento para recuperar control:

- **Proton Drive:** Almacenamiento cifrado en la nube de Proton. Similar a su correo, los archivos se cifran localmente y solo se descifran con la clave del usuario. Se accede por app o web, no hay cliente nativo Android aún (pero se puede usar el navegador o la app general de Proton). Migrar documentos a Proton Drive es un acto de soberanía: Google no puede leer ni indexar fotos o documentos, pues están encriptados. La implementación

implica subir archivos desde el móvil a través de la app y organizar carpetas. Contra la amenaza corporativa, se fortalece al romper la centralización, ya que nadie, salvo el usuario, tiene acceso a la llave de descifrado.

- **Disroot Cloud:** Usando Nextcloud en Disroot. Disroot ofrece instancias Nextcloud libres. Se accede instalando una app de Nextcloud o a través del navegador móvil. Tras iniciar sesión, se puede subir y sincronizar archivos (cloud docs, fotos). Al ser open source, el usuario puede incluso exportar datos o migrarlos a otro servidor fácilmente, garantizando autonomía de proveedor. Al usar Disroot en vez de Drive, los archivos van a un servidor cooperativo gestionado por voluntarios, disminuyendo el riesgo de uso indebido de datos. Configurar la app Nextcloud es directo: sólo se necesita la URL de Disroot y credenciales.
- **Tuta Drive:** Servicio de almacenamiento de Tutanota. Cifrado automático al subir archivos. La app de Tutanota incluye la opción de Drive. Toda la información (docs, fotos) se guarda cifrada y solo accesible a los dispositivos autorizados. Al usar Tuta Drive, cada archivo se protege frente al acceso de Tuta. Un usuario configura la aplicación de Tutanota y activa la sección de archivos. Esto contribuye a la resistencia porque incluso la metádata de los archivos (nombres) puede cifrarse; Google ya no tiene acceso a tus fotos personales en Drive.
- **kDrive:** La app kDrive de Infomaniak, disponible en F-Droid bajo licencia GPLv3, es una solución de nube soberana y código abierto, ideal para perfiles activistas, profesionales y uso cotidiano que priorizan la privacidad. Su arquitectura Android modular (MVVM, Kotlin) emplea Realm para caché offline y Room para tokens, garantizando eficiencia y seguridad local. La versión F-Droid elimina dependencias propietarias y telemetría de terceros (como Sentry), a diferencia de la versión estándar. Los datos se almacenan exclusivamente en centros suizos TIER III+, con cifrado AES-128-CBC en reposo y SSL/TLS en tránsito. Aunque no es zero-knowledge por defecto, su ecosistema soberano, sin análisis ni reventa de datos, ofrece una alternativa robusta, auditable y técnica frente a las big tech, permitiendo sincronización segura, colaboración y control total sobre la información sensible del usuario.
- **Tresorit:** Servicio de nube cifrada de extremo a extremo (base suiza). Tiene app Android robusta. Cada archivo subido se fragmenta y encripta localmente. Solo el usuario con la contraseña puede reconstruirlo. Instalar Tresorit y subir archivos (fotos, documentos) asegura que ningún empleado ni hackeo corporativo accederá a ellos. La desventaja es pago,

pero su ventaja en resistencia es máxima: funciona como una fortaleza personal de datos. Se usa igual que Drive: crea carpetas, arrastra archivos, comparte de forma protegida con otros usuarios Tresorit. Neutraliza cualquier amenaza de filtración masiva en la nube.

- **OwnCloud:** Software libre para crear nube personal. Requiere configurar un servidor (o usar uno ajeno). Hay apps Android oficiales para sincronizar archivos. Es la versión DIY de Drive. Al implementar OwnCloud (por ejemplo en un servidor casero o contratado), el usuario retiene control absoluto: la nube es local o en un servidor de confianza. Todo queda bajo jurisdicción propia. La configuración incluye habilitar la app, conectar con la URL del servidor, y seleccionar qué sincronizar. La autodefensa aquí es total: no hay empresa entre tú y tus datos. Google no ve nada de tu "Drive", pues solo tu servidor ve tus archivos.
- **Filen.io:** Plataforma de almacenamiento que funciona encriptando archivos en el navegador (y app) antes de subirlos. Tiene opción gratis limitada. Aunque no tan popular, es una capa de protección adicional: el proveedor no tiene la clave. Para usar Filen.io en el móvil, se accede vía web (o app si existe). Subir fotos/doctos garantiza una capa de separación: ni ellos pueden leer el contenido. Esto compite contra Google Drive al poner fuerte cifrado de lado del cliente.
- **Mega.nz:** Conocido por ofrecer 50 GB gratuitos, cifra archivos de extremo a extremo. Tiene app Android oficial. Cada usuario recibe una clave privada única. La resistencia radica en que MEGA no almacena llaves descifradoras de los usuarios (teóricamente). Al usarlo, los archivos sensibles permanecen cifrados en su nube. Configurarlo implica subir con app y administrar enlaces con contraseña si se quiere. Aunque Mega Store debut fue en NZ, su sede actual y prácticas han generado controversias, pero aún así aleja datos directos de Google.
- **Nextcloud:** Solución libre y autoalojada similar a OwnCloud. Tiene clientes Android bien desarrollados. Permite sincronizar archivos, calendario, contactos, notas, etc., todo cifrado opcionalmente por plugin (Nextcloud Encrypt). Implementar Nextcloud puede ser en tu propio servidor o en un proveedor de confianza. En la app se configura la URL y la cuenta. Con Nextcloud, el teléfono móvil puede respaldar fotos sin nunca utilizar las nubes comerciales. Es una defensa porque el código fuente es abierto y el usuario controla la infraestructura: nada puede ser monetizado sin su consentimiento.
- **Internxt:** Nube descentralizada con enfoque en privacidad (basada en blockchain). App disponible para Android. Divide archivos en fragmentos

cifrados y distribuidos en la red. El usuario guarda la clave privada. Eliminar Google Drive y pasar a Internxt significa que ni Google ni un único servidor saben qué archivos almacenas. La configuración es simple: crear cuenta e iniciar sesión en la app. La desventaja es espacio y dependencias novedosas, pero su objetivo es puramente privacidad. Neutraliza la vigilancia en la nube al fragmentar y cifrar todo.

Alternativas a Google Translate

Los servicios de traducción automática suelen requerir enviar textos a servidores externos. Estos proyectos ofrecen traducción sin depender exclusivamente de la infraestructura de Google:

- **TranslateYou:** Aplicación multilenguaje que integra varios motores (DeepL, Microsoft, Yandex) y proxies independientes. Es de código abierto y permite traducir sin registrar datos. Al usarla en Android (F-Droid), se introducen frases que son enviadas a los traductores elegidos, pero la app misma no guarda historial ni datos. Así se evita la recolección de Google sobre las consultas. Configurar esta app implica permitir acceso a Internet, pero con la confianza de que no registra localmente lo ingresado.
- **DeepL:** Conocido servicio de traducción superior en calidad. No es libre, pero tiene buena política de privacidad (EU). Ofrece app Android oficial. Se diferencia de Google Translate en que no construye perfiles del usuario; actúa como caja negra de traducción. Para la autodefensa, usar DeepL significa que tus textos viajan a Alemania, bajo RGPD, en lugar de a servidores de Google en EE. UU. En la app se ingresa el texto y recibe la versión traducida. Aunque no es totalmente libre, reduce la dependencia americana.
- **Lentil Translate:** Cliente Android de Lingva (front-end privado para Google Translate). Se basa en instancias públicas (o privadas) de Lingva, que traducen usando el motor de Google pero sin API oficial ni rastreo. Se instala desde F-Droid. Al enviar un texto, la petición pasa por Lingva, ocultando al usuario de Google. La ventaja: no necesitas ingresar a translate.google.com, y además la aplicación no guarda consultas. La configuración consiste en seleccionar la instancia preferida de Lingva (por ejemplo, lingva.ml). Esto combina la eficacia de Google Translate con la privacidad de no dar tu IP ni cookies a Google, fragmentando la ruta de datos.
- **Seamless:** Traductor offline de voz/texto basado en modelos ML (Seamless M4T). Descarga un gran modelo de traducción en el dispositivo

(multilenguaje). Una vez instalado, puede traducir sin conexión en varios idiomas. Esto elimina por completo la necesidad de enviar datos a la nube. Para implementarlo, al iniciarla la primera vez la app descargará el modelo (requiere Internet). Después, cualquier traducción de voz o texto se hace localmente, garantizando confidencialidad total. Desde la perspectiva de resistencia, usar Seamless significa tener un traductor sin enviar nada a Google; la red de datos corporativa se elude usando solo el procesador del móvil.

Alternativas a Google Chrome (Navegadores)

El navegador es una pasarela crítica. Estas alternativas se centran en tecnología libre y bloqueo de rastreadores:

- **IronFox:** Navegador móvil Android basado en Firefox (antiguo Mull Browser). Se enfoca en máxima privacidad y anonimato. Incorpora protección contra fingerprinting y tracking por defecto. Al instalarlo, cada vez que navegues la huella digital se dificulta, ya que bloquea componentes identificadores. Comparado con Chrome, IronFox no liga tu actividad a ninguna cuenta de Google, pues funciona al margen de servicios de Google. Se configura desactivando elementos como WebRTC, usando contenedores si están disponibles, etc. Su uso, por tanto, mitiga fuertemente amenazas de seguimiento y evita la integración intrínseca de los sistemas operativos móviles con Google.
- **WebLibre:** Navegador independiente construido sobre Gecko (motor de Mozilla). Proporciona separación de contexto mediante contenedores, encriptación de búsqueda local y un proxy Tor integrado por pestaña. Para instalarlo se descarga desde F-Droid o repositorios. En la configuración inicial se elige perfil de seguridad (por ejemplo, “Quick Start”). Esto habilita uBlock Origin automáticamente. Cada pestaña puede configurarse con aislamiento distinto (un dominio por contenedor), eliminando cookies entre ellas. Además, su buscador local impide enviar consultas a Google; en cambio el texto de búsqueda se procesa en el propio dispositivo. Todo ello intensifica la privacidad, ya que elimina la correlación cruzada entre sitios y oculta el historial dentro del propio navegador.
- **AOSmium**: AOSmium es el navegador y proveedor de WebView oficial de AXP.OS, diseñado como un fork de Chromium centrado en la seguridad y la autodefensa digital. Hereda el legado del proyecto Mulch de DivestOS, integrando rigurosos parches de endurecimiento provenientes de Vanadium (GrapheneOS) y Cromite para mitigar vulnerabilidades del

motor de renderizado. Su arquitectura prioriza la soberanía tecnológica mediante procesos de compilación automatizada (CI/CD) y la eliminación de anti-características, garantizando actualizaciones rápidas frente a los Boletines de Seguridad de Android (ASB). Como medida de protección proactiva, deshabilita por defecto la compilación JIT, reduciendo drásticamente la superficie de ataque ante exploits de ejecución de código. Al operar como un componente del sistema verificable y de código abierto, AOSmium resguarda la privacidad y fortifica la integridad de toda la pila de aplicaciones, ofreciendo una defensa robusta contra la vigilancia digital.

- **FOSS Browser:** Navegador de código abierto con UI Material y barra inferior para facilidad de uso con una mano. Incluye AdBlock integrado y perfiles de privacidad personalizables (puedes desactivar JavaScript, cookies de terceros, huellas digitales, etc., por dominio). Tras instalarlo (F-Droid), se crean perfiles ("Protegido" o "Confiable") que se asignan a sitios. La ventaja frente a Chrome es que el usuario controla todo nivel de bloqueo: por ejemplo, un perfil puede impedir toda ejecución de scripts. No hay sincronización con Google; toda personalización se guarda localmente. Esto contrarresta la recopilación de datos porque el navegador impide activamente medios de rastreo comunes. La configuración de listas negras y permisos de sitio es guiada y transparente, reduciendo el peligro de rastreadores ocultos en páginas web.
- **Brave Browser:** Basado en Chromium pero con bloqueo de anuncios y trackers por defecto. Su instalación es fácil desde Google Play o F-Droid. Brave desconecta de Google agregando su propio buscador (Brave Search) y bloqueando scripts de seguimiento. Además, cuenta con HTTPS Everywhere y fingerprinting protection. Al usar Brave, la navegación web deja de reforzar el algoritmo publicitario de Google; por el contrario, muchos sitios simplemente muestran espacios en blanco en lugar de anuncios. Esto da al usuario más privacidad. Cabe señalar que Brave introduce su propio sistema de micropagos (BAT), pero es opcional. En términos de resistencia, Brave es un medio término: por un lado usa código Chromium; por otro lado se esfuerza en romper con el modelo de anuncios invasivo. Configurarlo implica revisar las configuraciones de privacidad y bloquear incluso más si se desea.
- **Cromite:** Navegador enfocado en la privacidad, fork de Bromite (que a su vez es fork de Chromium). Ofrece bloqueo de ads/trackers y ajustes para minimizar la integración con Google. Se descarga vía F-Droid (o web oficial). Incluye soporte para extensiones y UserScripts, siendo tan rápido como Chrome. Para la autodefensa digital, al usar Cromite un usuario no

renuncia a la velocidad de Blink, pero añade fuerte protección. Permite deshabilitar fácilmente servicios de estadísticas de Google y desactivar prefetching de DNS. Configurarlo con cuidado (por ejemplo, activar la protección contra huellas digitales) refuerza la privacidad. En efecto, Cromite busca ofrecer la misma experiencia sin los hábitos ocultos de Google, mitigando la amenaza de acciones telefónicas automatizadas (como el reCAPTCHA) vigiladas por el navegador.

En conjunto, estas alternativas limitan la capacidad de Google de supervisar la navegación web, ya que rompen la integración del navegador con los servicios de la empresa y evitan la ejecución de scripts ajenos.

Alternativas a Google Maps

Los mapas libres proveen navegación sin depender de la cartografía de Google. Basados en OpenStreetMap y con funciones offline, reducen la fuga de ubicación:

- **OsmAnd:** Aplicación muy popular de mapas offline de OSM. Se instala desde F-Droid y se descargan los mapas de las regiones deseadas (usa relativamente poco espacio gracias a vectorización). Ofrece navegación GPS para autos, bici, a pie, rutas a puntos y capas (por ejemplo, senderos de montaña). Su uso garantiza que ninguna consulta de ruta o ubicación se envíe a Google. Al configurar OsmAnd, se puede activar también la navegación por voz y elegir entre visualizaciones (satélite, topográfico). Toda la cartografía es local, por lo que ni siquiera se generan registros centrales de ubicaciones. Es autodefensa pura: tu teléfono sabe dónde estás y adónde vas sin informar a corporaciones.
- **Gmaps WV**: GMaps WV es un contenedor WebView de código abierto en F-Droid que permite usar Google Maps sin exponer datos nativos del dispositivo. Su arquitectura actúa como capa de aislamiento, bloqueando rastreadores de Google y recursos de terceros, y restringiendo todas las solicitudes de red exclusivamente a HTTPS. Funcionalmente, ofrece mapas con direcciones paso a paso (sin navegación en tiempo real), permitiendo alternar manualmente los permisos de ubicación. Para proteger la privacidad, elimina datos privados al cerrarse, mitigando la huella digital persistente. A pesar de limitaciones técnicas inherentes a WebView, como la imposibilidad de bloquear WebRTC o el vaciado automático de caché por optimización de recursos, su diseño prioriza la soberanía del usuario, el cifrado en tránsito y la minimización de datos, siendo una herramienta robusta para activistas y usuarios conscientes.

- **Organic Maps:** Basado en los creadores de Maps.me, es una app de mapas offline centrada en actividades al aire libre. Como OsmAnd, descarga mapas OSM. Brilla en rutas de senderismo, ciclismo y también funciona de noche. Se instala y se configuran regiones a usar. Todo es local: búsquedas de lugares, cálculo de rutas y POIs no requieren internet tras la descarga inicial. En términos de resistencia tecnológica, implicar a Organic Maps es eliminar la recogida de datos de Google: tus desplazamientos de peatón o campamento ya no nutren ningún servicio de ubicación global. Además, la app confirma explícitamente su rechazo a la telemetría.
- **Geolibre:** GeoLibre es una plataforma GIS móvil de código abierto para Android (Tauri v2, Rust y React) que destaca por su procesamiento geoespacial local en un paquete de solo 40 MB. Sus herramientas clave incluyen análisis vectorial avanzado mediante WebAssembly (DuckDB-WASM y Pyodide), gestión autónoma de formatos como GeoJSON y GeoParquet, y un asistente de IA integrado. Funcionalmente, opera bajo un modelo de privacidad de confianza cero y sin telemetría, ejecutando todas las operaciones sensibles directamente en el dispositivo para garantizar la absoluta soberanía de los datos. Optimizada técnicamente para el Android moderno (API 36 y alineación de memoria de 16 KB), ofrece una solución robusta, ética y resistente para el mapeo de campo y la acción colectiva, eliminando por completo la dependencia de servidores externos.
- **CoMaps:** Navegación comunitaria basada en OSM. Permite ver mapas offline, buscar lugares y obtener rutas básicas. Instalar CoMaps garantiza que se lean datos de una base de datos descentralizada y no de Google. Usa también OpenStreetMap y no rastrea ni envía la ubicación del usuario a terceros. Al activarlo en Android, las capas que se bajen se mantienen locales. Como con Organic Maps, cualquier ruta creada con CoMaps ocurre sin compartir datos. Para autodefensa, reduce la exposición a vigilancia de movilidad: el proveedor de CoMaps no almacena dónde viajaste ni con quién compartiste destino, a diferencia de Google que podría inferir cosas sensibles a partir de ello.

Alternativas a Google News (agregadores de noticias)

En lugar de un algoritmo centralizado, estas apps permiten suscribirse a canales RSS, dando al usuario pleno control editorial:

- **Readify:** Lector RSS Android local. No sincroniza con servicios externos: descarga directamente los feeds que configures. Se instala como APK o vía repo alternativo. En la configuración se añaden URLs de RSS de sitios de

noticias o blogs. El usuario obtiene las noticias actualizadas en su dispositivo, sin pasar por servidores de Google. Esto contrarresta el sesgo algorítmico de Google News: el propio usuario escoge las fuentes y decide qué leer. Además, la app no reporta métricas a terceros ni indexa tu comportamiento. Para implementarlo eficazmente, importa archivos OPML (con listas de feeds) y ajusta la frecuencia de actualización.

- **Feeder:** Aplicación de feeds RSS/Atom que se sincroniza con servicios (pero también funciona localmente). De código abierto y actualizada. Se instala desde F-Droid o Play y luego se añaden feeds. Admite tags y carpetas para ordenar noticias. A nivel estratégico, usar Feeder significa evitar abrir Google News: la curación de contenidos la realiza uno mismo. Configurar la sincronización con FreshRSS o Feedly (opcional) posibilita backup en nube privada; pero el punto es que la lectura en sí permanece libre de algoritmos ajenos.
- **Nunti:** Lector RSS con diseño moderno. Destaca por aprendizaje adaptativo: la app resalta más las noticias relacionadas con temas previos leídos. Se instala y se añaden fuentes RSS a mano. Su sistema local de "preferencias de lectura" permite cierto filtrado de temas sin compartir nada en la red. Con Nunti, se puede filtrar feeds por categorías. Esto resiste la centralización al no mandar tus lecturas a ninguna entidad: toda la inteligencia está en el dispositivo.
- **FeedFlow:** Aplicación multiplataforma (incluye Android) enfocada en un timeline simple. Mantiene el orden cronológico puro y admite sincronizar con servicios propios (FreshRSS, Miniflux, etc). Al instalar FeedFlow, se importa tu lista de feeds y automáticamente se crea una línea de tiempo limpia. Su naturaleza cross-platform e interoperabilidad hace que un usuario no tenga que depender de Google News en ningún dispositivo. Configurar FeedFlow puede implicar activar Dropbox o Google Drive para respaldos (optativo) o mejor usar un servidor libre como FreshRSS para evitar Google por completo. En resumen, FeedFlow da al usuario la libertad de leer cualquier fuente RSS de manera uniforme, neutralizando los monopolios de agregación de noticias.
- **Neo Feed, Capy Reader, Readrops, Read You:** Estas apps comparten la filosofía RSS. Cada una tiene su estilo: Neo Feed es ligera y ordenada, Capy Reader permite sincronización con servicios como Feedbin o FreshRSS, Readrops maneja múltiples cuentas (Fever API, Nextcloud News), y Read You aplica Material You a la experiencia RSS. Todas se instalan y configuran añadiendo las URL de los feeds deseados o sincronizando con servidores propios. Funcionan offline y no tienen publicidad. Su uso

combate la desinformación y la censura algorítmica: al usar RSS directamente, el usuario decide qué medios consultar. Además, al ser software libre, ninguna telemetría corporativa se ejecuta. En conjunto, estos lectores son herramientas de resistencia al proveer acceso directo a la información, sin intermediarios corporativos que decidan qué se muestra.

Alternativas a Gboard (teclados)

Gboard recopila pulsaciones para mejorar el diccionario de Google. Las alternativas listadas son teclados libres y simples:

- **FlickBoard:** Teclado libre con gestos (flicks) para escribir palabras rápidamente. Soporta varios idiomas y correcciones locales sin enviar nada a la nube. Al instalarlo, se debe activar en Ajustes → Teclado. Una vez activo, todo lo que escribas se queda en el dispositivo. Evita que Google sepa tus patrones de escritura o datos sensibles.
- **Urik:** Teclado minimalista enfocado en privacidad, parte del proyecto Replicant/Lineage. Solo ofrece textos sin sugerencias avanzadas. Instalado de F-Droid, no solicita conexión. Al usarlo, escribes sin autocompletar de Google, eliminando el envío de registros a servidores externos.
- **Fossify Keyboard:** Teclado de código abierto con énfasis en ser ligero y privado. Incluye autocorrección básica offline. Al activarlo en Android, todo el aprendizaje ortográfico se almacena localmente. Ayuda a la soberanía porque no comparte tu vocabulario personal con Google.
- **Simple Keyboard:** Una app ultra-básica: solo tecleo y punto. No tiene diccionario ni conexión. Se instala y habilita: no recopila nada, solo envía caracteres a cualquier app. Funciona sin restricciones (necesita permiso de Internet si no está el InternetPermissless mod). Su uso es la forma más elemental de resistencia: no provee predicciones ni envía datos.
- **HeliBoard:** Diseñado para usarse con una mano (teclado vertical). Sin predicciones en la nube. Se instala, se selecciona el idioma, y ya. Al escribir con él, no se crea historial transferible; el objetivo es disminuir la entrada de datos a terceros.
- **CleverKeys, Tiny Keyboard, FUTO Keyboard:** Teclados pequeños y de un solo panel. Cada uno diseñado para máxima simplicidad (uno solo muestra una fila de teclas principales, otro agrupa letras por color). Al usarlos se minimizan los permisos (generalmente solo vibración) y se elimina cualquier operación en la nube. Por ejemplo, FUTO (Foldable Ultrasmall) incluso detecta gestos de plegado para activar el teclado. Usar estos

teclados significa renunciar a comodidades de escritura rápida en favor de privacidad absoluta.

- **CleverKeys:** CleverKeys es un teclado Android de código abierto (GPL-3.0) en F-Droid, diseñado para usuarios avanzados con enfoque absoluto en la privacidad. Funciona 100% fuera de línea (sin permisos de red), eliminando telemetría, analíticas o sincronización en la nube, garantizando que los datos nunca salgan del dispositivo. Su motor de escritura por deslizamiento y autocorrección usa un modelo neuronal Transformer (ONNX, ~13MB) que se ejecuta localmente con aceleración XNNPACK, evaluando diccionarios de hasta 15 idiomas simultáneamente. Incluye un portapapeles ilimitado con exclusión para gestores de contraseñas, búsqueda regex, edición en línea y gestión de tareas, además de 208 acciones de deslizamiento corto personalizables. Al ser completamente auditable, sin dependencias externas y con personalización profunda (temas, diseños XML), ofrece soberanía digital total, ideal para activistas y profesionales que priorizan la seguridad.
- **Tiny Keyboard:** Un teclado muy reducido para pantallas pequeñas.
- **FUTO Keyboard:** Ideal para móviles con pantallas muy pequeñas o uso de una mano, porque ocupa solo una parte de la pantalla y se colapsa con un gesto.
- **Cada uno**: evita la recopilación de IA de pulsaciones. Configurarlos implica activarlos en la configuración de idioma de Android y elegirlos como teclado predeterminado. Luego, las sugerencias ortográficas se calculan localmente o no existen, impidiendo que Google analice lo que escribes.

Alternativas a Google Meet (videoconferencias)

Reunirse en línea sin los servicios de Google implica plataformas descentralizadas o privadas:

- **Jitsi Meet:** Plataforma de videoconferencia libre y descentralizada. Funciona por navegador o app Android. No requiere registro (utiliza salas únicas). Instalar la app de Jitsi (disponible en F-Droid) y crear una sala genera un enlace. Los datos de video/audio no pasan por Google: los servidores de Jitsi (propios o comunitarios) se encargan del enrutamiento. Con cifrado de extremo a extremo opcional, Jitsi evita que Google vigile tus reuniones. Es especialmente útil para grupos, activistas o comunidades que buscan evitar la plataforma de Google y su potencial vigilancia de los contenidos de llamadas.

- **Nextcloud Talk:** Módulo de Nextcloud para videollamadas. Si se tiene un servidor Nextcloud (autohospedado o un proveedor de confianza), Nextcloud Talk se activa. En Android se instala la app Nextcloud Talk y se configura con la URL del servidor. Las reuniones se cifran en los servidores propios, manteniendo confidencialidad. A nivel estratégico, usar Talk significa que las transmisiones de video quedan bajo tu infraestructura, no en manos de Google. Cualquiera puede poner su instancia; para el usuario, basta con invitar participantes a unirse desde la app Nextcloud. Esto elimina el riesgo de que Google registre metadatos de tus conferencias (p.ej. quién habló con quién).
- **Proton Meet:** Servicio de videollamadas del ecosistema Proton. Ofrece cifrado de extremo a extremo sin necesidad de registro (o usando cuenta Proton). Es reciente pero funciona directamente desde el navegador; para Android, usa la app ProtonDrive con pestaña de Meet o se adapta la web. Al invitar, Proton Meet genera una sala. Los datos fluyen cifrados entre participantes y los servidores suizos. Aunque aún se basa en el backend de Jitsi, la diferencia es que Proton cumple con su política de no registro. Al elegir Proton Meet, se opta por una llamada encriptada bajo ley suiza, evitando que Google (o cualquier otro) almacene quién estuvo en la llamada.
- **KMeet:** kMeet de Infomaniak, disponible en F-Droid y con código abierto en GitHub bajo licencia GPL-3.0, es una solución de videoconferencia basada en Jitsi Meet que prioriza la soberanía digital. Alojada íntegramente en la nube suiza (Ginebra), protege a usuarios, activistas y ONGs de legislaciones extraterritoriales como el CLOUD Act. Técnicamente, ofrece cifrado de extremo a extremo, cero telemetría, sin requerimiento de cuentas ni correos para unirse, y salas protegidas por contraseña. Su arquitectura abierta garantiza auditoría completa, independencia de ecosistemas propietarios y resistencia a la vigilancia masiva. Al combinar la infraestructura ética de Infomaniak con la federación de Jitsi, kMeet proporciona una alternativa robusta, segura y accesible para comunicaciones cotidianas o de alto riesgo, asegurando confidencialidad, integridad de datos y control total sobre la identidad digital sin depender de grandes corporaciones tecnológicas.
- **Mumla:** Servicio gratuito de videollamadas cifradas en Estonia. No requiere instalación; se usa web. Para Android, se puede abrir en navegador. Ofrece salas privadas con contraseñas. Toda la comunicación se cifra E2EE (basado en el protocolo WebRTC) lo que impide que terceros la oigan. Al usar Mumla, se elimina la necesidad de Google Meet o Zoom:

basta compartir la URL de la sala. La ventaja en soberanía es que los servidores de Mumla no guardan contenido; las claves de llamada residen localmente en los navegadores de cada usuario. Esto protege las reuniones de “escuchas corporativas”.

Alternativas a Google Authenticator (2FA)

Las aplicaciones de autenticación generan códigos de un solo uso; estas alternativas promueven la independencia:

- **Proton Pass:** Aunque principalmente gestor de contraseñas, incluye función de autenticación de dos factores. Almacena tus códigos 2FA cifrados junto a otras credenciales. Se instala la app Proton Pass en Android y se importan los secretos (p.ej. escaneando QR). Los códigos se generan localmente, sin conexión. No usa proveedores externos de datos, por lo que Google no puede registrar tus movimientos en estas apps. La ventaja es todo es cifrado de extremo a extremo.
- **Proton Authenticator:** Aplicación independiente de Proton para 2FA. Similar a TOTP convencional. Se instala desde la tienda de Proton. Configurar cuenta implica escanear los códigos QR de los servicios. Cualquier código generado es interno de la app. Los beneficios son idénticos a Proton Pass (resistencia corporativa y cifrado), pero en forma de app dedicada.
- **Conceal:** Aplicación open source para generar códigos TOTP y HOTP. Se instala en Android desde F-Droid. No guarda información en la nube; las llaves se almacenan localmente o con opción de respaldos cifrados. En la configuración, se añaden claves manualmente o escaneando. No requiere permisos extra, garantizando que el Google Play Services no intervenga. Cada vez que inicies sesión en servicios con 2FA, tu teléfono generará el código sin poner datos sensibles en riesgo.
- **Tokn:** Autenticador moderno con diseño Material. Permite insertar tokens y exportar/respaldar con cifrado. Disponible en tiendas de apps. Funciona desconectado. Al instalarlo, se añaden tokens como en otras apps 2FA. Los datos se pueden cifrar con contraseña. Su contribución a la soberanía es que es una app comunitaria (SUIZA originaria) que no vincula tus códigos a cuentas de Google.
- **Reloado:** Autenticador sencillo pero enfocado en privacidad. Se encuentra en F-Droid y tiendas. No persiste datos en la nube, todo local. Su configuración básica (agregar TOTP) garantiza que Google no intervenga en el proceso 2FA.

- **Ente:** Solución de software libre basada en PGP para 2FA (similar a OTP pero con claves PGP). Se instala en Android (requiere conocimientos técnicos). Funciona generando firmas de desafíos, por lo que ni siquiera comparte la clave secreta con el servicio, aumentando privacidad. Su uso concreto es complejo, pero ante la soberanía tecnológica, supone una forma de dos factores "autónoma" sin depender de servidores centrales.
- **Aegis:** Authenticator libre popular. Integra importación/exportación cifrada. Se instala de F-Droid. Cada código se genera localmente. Se puede proteger con contraseña para impedir que la app sea abierta por cualquiera. Evita el vínculo con servicios externos.
- **Pocket2FA:** Otro cliente TOTP open source. Similar a Authy pero offline. Al instalar, se añaden tokens. Exporta claves de manera segura. Colabora con la resistencia al evitar que la cuenta Google pueda ser factor de identificación.
- **FLauth:** Cliente sencillo TOTP/FIDO. Se instala desde F-Droid. Dispone de cifrado de base de datos local. Tras añadir cada token, solo la app conoce la clave secreta. De esta forma, la autenticación en otros servicios sigue siendo posible sin entregar información sensible a Google.
- **FreeOTP:** Iniciador de OATH de Red Hat. Extremadamente básico: genera códigos TOTP basado en la clave secreta. No guarda información personal, no hay nube. Instalar FreeOTP y configurar los tokens significa mantener la autenticación fuera de los ecosistemas corporativos.
- **MAuth:** Gestor de autenticación de IU moderna (Material). Funciona sin nube y es open source. Tras instalarla (F-Droid), se configuran tokens TOTP. Usarla constituye un movimiento para dispersar la confianza: con MAuth ninguna gran compañía recibe metasobre cada intento de login, ya que la validación se hace totalmente en tu propio dispositivo.

Alternativas a Google Gemini (IA)

Llaman "IA" a diversos asistentes inteligentes. Estos servicios proponen la interacción con inteligencia artificial sin servir a Google:

- **Proton Lumo:** Asistente de Proton (en desarrollo), integrado a Proton Chat. Promete generar respuestas sin datos de usuario. Aún no ampliamente disponible, pero su futura adopción permitirá a los usuarios experimentar IA (p.ej. GPT) sin alimentar motores de Google. Guardará las consultas encriptadas en servidores suizos y se integrará con la suite Proton. Su filosofía rebelde es enfocar la IA como herramienta privada, no como un medio de vigilancia.

- **Kai 9000:** Supongo que se refiere a alguna app de IA. En el contexto, podría ser un chatbot local o basado en servidores libres (no hay info clara). Si existiera, sería un asistente de código abierto que se ejecuta en el dispositivo o usa API públicas. Su implementación implicaría ingresar preguntas sin autenticarte con Google. Actuaría como laboratorio de IA personal sin filtrar tus datos a gigantes.
- **GPTmobile:** Versión móvil (posiblemente no oficial) de modelos de lenguaje GPT. Instalaría un cliente que conecta a la API de OpenAI u Open Source. La ventaja en soberanía sería mínima si usa OpenAI, pero al menos no es Google. Se configuraría con tu propia clave API. Como resistencia, apuntaría a no usar Google Bard o Gemini, en vez apostar por alternativas similares de terceros.
- **Maskan:** Desconocido para mí en IA. Posible herramienta comunitaria de chat similar a ChatGPT. Si existe, su uso implica acceso a modelos grandes en servidores propios. Sería un acto de defensa si usara modelos open source (llama, etc) detrás.
- **Agora, Oxproxion, ChatAir, ChatterUI, DuckAssist:** Básicamente, son nombres de apps de chat GPT, Claude, Gemini y mucho más libres, seguras, respetuosas con la privacidad del usuario y sin el seguimiento y telemetría de OpenAI, Anthropic, etcétera. Su instalación variaría, pero todas buscarían reemplazar a Google Assistant, Gemini, ChatGPT o Claude con IA generativa. Su doctrina de soberanía es apostar por software comunitario (quizás adaptado de GPT-3.5/4) en vez del modelo cerrado de Google. Al usarlas, el usuario acepta que su interacción de lenguaje no pase por Google, liberando la conversación de algoritmos de Google. En la práctica, cada app requerirá dar una API key (por ejemplo de Gemini o Claude), manteniendo así la propiedad de los datos. Configurarías la API en la app y listo.
- **DuckAssist:** DuckAssist es un contenedor WebView ligero, de código abierto (GPL-3.0) y disponible en F-Droid, diseñado para interactuar con Duck.ai priorizando la soberanía de datos. Su arquitectura en Java y HTML elimina dependencias de servicios propietarios, integrándose como asistente digital predeterminado con activación por voz y menú contextual para consultar texto seleccionado desde cualquier aplicación. Protege la privacidad mediante la purga automática de caché al cerrar, persistencia de sesión controlada y aislamiento de navegación: los enlaces externos se redirigen al navegador del sistema, evitando el rastreo dentro del chat. Al no incorporar telemetría ni SDKs de terceros, garantiza que las interacciones con IA permanezcan confinadas, ofreciendo una experiencia

fluida, segura y alineada con principios de cifrado, auditoría técnica y resistencia digital frente a ecosistemas cerrados.

- **AIyo**: AIyo es una aplicación Android de código abierto disponible en F-Droid que fortalece la autodefensa digital mediante una arquitectura BYOK (Bring Your Own Key) para conectar con modelos de IA vía OpenRouter. Su desarrollo en Kotlin con arquitectura MVVM asegura transparencia y auditabilidad, eliminando telemetría y garantizando que la app no recopila datos del usuario. Este enfoque otorga soberanía tecnológica: el usuario controla absolutamente sus claves API y flujos de información, previniendo el vendor lock-in y la minería de metadatos. Al desacoplar la interfaz del proveedor de IA, Aiyo defiende la privacidad y los datos personales en escenarios de riesgo (activismo, profesional o cotidiano), permitiendo razonamiento y búsqueda web sin sacrificar la confidencialidad, cumpliendo así rigurosos criterios técnicos de seguridad, código abierto y resistencia digital.
- **AI Hub**: AI Hub, disponible en F-Droid, es una aplicación Android de código abierto (GPL-3.0) que agrega múltiples asistentes de IA en una interfaz unificada, diseñada bajo principios estrictos de soberanía y autodefensa digital. Su arquitectura "privacy-first" garantiza la protección de datos personales al bloquear por defecto anuncios y rastreadores mediante la lista de hosts de StevenBlack, eliminando telemetría, analytics o cualquier recopilación de información identificable. Al ser completamente verificable, permite a usuarios y organizaciones auditar o compilar su propio código, asegurando independencia de ecosistemas propietarios y control total sobre las sesiones persistentes. Esta herramienta fortalece la seguridad digital al ofrecer un entorno limpio, personalizable y sin distracciones, donde la privacidad es la base estructural de cada interacción con servicios de IA externos.

Alternativas a Google Keep (Notas)

En la gestión de notas, evitar Google implica elegir apps cifradas o autocontenidas:

- **Linwood Flow:** Aplicación de notas sencilla y gratuita. No conecta con servidor alguno y su base de datos se mantiene en el dispositivo (o en storage encriptado del usuario). Se pueden crear listas y dibujos básicos. La autonomía proviene de que ningún dato sale del teléfono. Al instalar Flow, cada nota queda encerrada localmente (se respalda en Google Drive solo si

el usuario lo hace manualmente). Esto evita filtrado corporativo de texto escrito.

- **Butterfly:** Notas minimalista con almacenamiento local. Almacena todos los apuntes en un archivo SQLite en el dispositivo, sin sincronización predeterminada. Puede activarse Auto-backup en local (encontrándose solo en el teléfono). Su filosofía es concentrarse en el dispositivo. Al usarla, tus ideas, tareas, apuntes y listas no atraviesan internet, eliminando el riesgo de que Google los analice para publicidad, seguimiento o recolección de datos.
- **Flux:** Flux es una app de productividad Android de código abierto (GPL-3.0) en F-Droid, construida con arquitectura MVI, Kotlin y Jetpack Compose. Su diseño "offline-first" emplea la base de datos local Room, asegurando que notas, tareas y hábitos se procesen íntegramente en el dispositivo, neutralizando riesgos de filtración en la nube. Protege la privacidad mediante cero recolección o transmisión de datos a terceros, reforzada con bloqueo biométrico y protección de pantalla. El permiso de internet solo se usa para renderizar multimedia en Markdown, mientras recordatorios y notificaciones se gestionan localmente. Su código auditable, independencia de ecosistemas propietarios y almacenamiento local la consolidan como una herramienta robusta para activistas y profesionales que exigen soberanía de datos, seguridad avanzada y resistencia digital, manteniendo una interfaz Material 3 fluida y personalizable.
- **Leafpad:** Leafpad es una aplicación de notas de código abierto en F-Droid, con arquitectura local-first que garantiza la soberanía de datos. Funciona completamente offline, sin requerir internet, cuentas ni permisos invasivos, eliminando riesgos de telemetría o filtración a servidores externos. Desarrollada en Java, almacena la información exclusivamente en el dispositivo y la elimina por completo al borrarse, dificultando recuperaciones forenses. Incluye atajos de creación, modo oscuro, búsqueda, categorización y ocultamiento de notas. Al carecer de dependencias de ecosistemas propietarios y operar de forma autónoma, Leafpad es una herramienta robusta para la resistencia digital cotidiana, priorizando la privacidad, la mínima huella digital y el control absoluto del usuario sobre su información personal sin sacrificar usabilidad.
- **Joplin:** Aplicación poderosa de notas. Puede funcionar offline y con sincronización opcional a servicios de nube privados (Nextcloud, Dropbox). Toda la información se cifra end-to-end si se activa. Para la autodefensa, Joplin es crucial: el usuario puede autohospedar el servidor (Nextcloud) y sincronizar notas cifradas de extremo a extremo. La instalación de la app

en Android permite crear notas, álbumes y recordatorios. Si no se sincroniza, queda local. Su uso sustituye a Keep al asegurarse que las notas personales no se almacenan en Google y permanecen cifradas.

- **PocketPlan:** PocketPlan es una aplicación Android de código abierto (licencia MIT) disponible en F-Droid, diseñada para gestionar tareas, notas, compras y recordatorios sin comprometer la privacidad. Su arquitectura es estrictamente local: carece de permisos de internet, telemetría, rastreo o publicidad, garantizando la soberanía total de los datos. Funcionalmente, ofrece clasificación automática, personalización profunda y exportación de copias de seguridad locales, facilitando la migración y el respaldo autónomo sin dependencias de nubes propietarias. Desde una perspectiva de seguridad avanzada, su modelo de permisos mínimo (solo alarmas y notificaciones) reduce drásticamente la superficie de ataque. Esto la hace ideal para escenarios activistas, profesionales o cotidianos que exigen protección robusta mediante almacenamiento local y auditoría transparente de su código en GitHub, asegurando independencia digital y control absoluto sobre la información personal.
- **Standard Notes:** App de notas cifrada enfocada en privacidad. Todo se encripta y se sincroniza (si se desea) en servidores de Standard Notes. Instalarla en Android implica crear una cuenta en sus servidores (cifrados) o usar la versión local sin cuenta. Ofrece extensiones para calendario, editor markdown, etc. Su ventaja en soberanía es grande: todas las notas (texto, contraseñas, etc) quedan encriptadas a nivel de cliente. Es un fuerte contrapeso a Google Keep, porque incluso si se sincroniza, quien las almacena nunca las puede leer.
- **CipherNotes:** Ciphernotes (F-Droid/GitHub, licencia AGPL-3.0) es una app de notas "local-first" con cifrado de extremo a extremo (E2EE) del lado del cliente. Garantiza que cada nota se cifra antes de salir del dispositivo, almacenando solo texto cifrado en el servidor y protegiendo los datos durante la sincronización. Su gestión de claves permite compartir el cifrado de forma segura entre dispositivos mediante códigos QR, sin necesitar contraseñas. Técnicamente, su arquitectura abierta elimina rastreadores y soporta autoalojamiento (self-hosting) vía Docker, otorgando soberanía total sobre la infraestructura backend. Este enfoque descentralizado y de código abierto la hace ideal para activistas, profesionales y usuarios que priorizan la confidencialidad, la resistencia digital y la protección absoluta de su privacidad frente a ecosistemas propietarios.

- **CrystalPad:** Crystalpad es una aplicación de notas minimalista y de código abierto (licencia GPL-3.0) para Android, construida con Jetpack Compose y Material 3, diseñada para garantizar la soberanía de datos. Su arquitectura "Privacy First" elimina por completo los permisos de internet, el rastreo y la recolección de datos, mitigando riesgos de fuga para activistas, profesionales y usuarios cotidianos. Almacena la información exclusivamente de forma local mediante una base de datos Room, evitando sincronizaciones en la nube no verificadas. Además, integra autenticación biométrica para blindar el acceso, asegurando que las notas permanezcan inaccesibles ante extracciones físicas o accesos no autorizados. Al estar disponible en F-Droid y ser totalmente auditable, ofrece transparencia operativa, permitiendo a organizaciones y particulares mantener registros sensibles con independencia total de ecosistemas propietarios y telemetría invasiva.
- **QuickNotes:** QuickNotes es una app de notas de código abierto (Apache 2.0) que prioriza la soberanía de datos manteniendo la información estrictamente en el dispositivo, eliminando riesgos de telemetría o filtraciones en la nube. Su arquitectura MVC en Kotlin garantiza un funcionamiento auditable, ideal para activistas o profesionales que exigen confidencialidad crítica. Ofrece gestión local de notas con búsqueda, etiquetas y recordatorios. La única conexión externa es opcional: el etiquetado por IA requiere una clave API propia, impidiendo que terceros intercepten contenido. Al carecer de dependencias propietarias, rastreadores o permisos excesivos, y ser compilada reproduciblemente por F-Droid, asegura integridad binaria y resistencia a la censura, protegiendo los datos personales mediante aislamiento local y control absoluto del usuario sobre su infraestructura digital.
- **EasyNotes:** EasyNotes es una aplicación minimalista de código abierto (GPL-3.0) disponible en F-Droid, desarrollada en Kotlin con arquitectura Jetpack Compose MVVM. Su diseño prioriza la privacidad y la soberanía de datos: opera con almacenamiento estrictamente local, cero telemetría, sin rastreadores y sin permisos obligatorios, auditando su seguridad directamente desde su repositorio GitHub. Incluye una bóveda de notas cifrada y bloqueo biométrico opcional, protegiendo información sensible de activistas, profesionales y usuarios cotidianos frente a ecosistemas propietarios. Soporta Markdown completo (con imágenes) y tema Material You, garantizando una experiencia fluida y autónoma. Al estar verificada en F-Droid, su código es 100% auditable, asegurando la ausencia de puertas traseras y consolidándola como una herramienta técnica, robusta e

independiente para la resistencia digital y la gestión segura de datos personales sin dependencias en la nube.

- **NotallyX:** NotallyX es una aplicación de notas minimalista, de código abierto (licencia GPL-3.0) y disponible en F-Droid, diseñada para maximizar la privacidad y la soberanía de datos. Almacena toda la información localmente, garantizando que las notas nunca salgan del dispositivo, eliminando riesgos de vigilancia en la nube, ideal para activistas y profesionales. Ofrece bloqueo biométrico o por PIN con cifrado de base de datos, además de copias de seguridad automáticas opcionalmente protegidas por contraseña. Carece por completo de anuncios, rastreadores o analíticas, reduciendo la telemetría a cero. Soporta texto enriquecido, listas de tareas, archivos adjuntos y recordatorios, con importación desde Google Keep o Evernote, facilitando la migración desde ecosistemas propietarios. Su arquitectura transparente y auditable permite a usuarios técnicos verificar su seguridad, ofreciendo un equilibrio robusto entre funcionalidad avanzada y protección integral de datos personales.
- **StyncyNotes:** Aplicación de notas con sincronización opcional (FOSS). Permite usar Nextcloud/Dropbox/ownCloud, etc. Configurarlo logra que tus notas se sincronicen en tu servidor seguro, manteniendo la soberanía. Al no depender de Google Drive, mantienes la soberanía de la información escrita. Se instala la app y se enlaza al servidor preferido.
- En resumen, cualquiera de estas apps reemplaza Google Keep evitando el espionaje corporativo. Al elegir gestores de notas cifrados o locales, se evita que Google acceda a pensamientos personales, aumentos y esquemas. Configurar estas apps consiste en habilitarlas como predeterminadas para notas o respaldar a nube privada, y así se cristaliza la soberanía sobre la escritura personal.

Alternativas a Google Fit (apps de salud y ejercicio)

Las aplicaciones de salud almacenan datos sensibles. Estas opciones proporcionan seguimiento físico sin alimentar a Google:

- **LibreFit:** LibreFit es un rastreador de ejercicios de código abierto (GPLv3) disponible en F-Droid, diseñado con una arquitectura "offline-first" que garantiza la soberanía total de los datos. Al no requerir registro, ni incorporar telemetría, analíticas o publicidad, elimina cualquier riesgo de exfiltración de información a terceros, siendo ideal para escenarios de alto riesgo como el activismo o el uso profesional que exige independencia de

ecosistemas propietarios. Toda la información (rutinas, series, repeticiones y progreso) se almacena exclusivamente de forma local en el dispositivo. Técnicamente, construido en Kotlin con Jetpack Compose, ofrece builds reproducibles que permiten verificar la integridad del código. Su dataset de más de 800 ejercicios funciona sin conexión, proporcionando una alternativa robusta, auditable y segura para usuarios y organizaciones que priorizan la privacidad radical y la resistencia digital frente a la vigilancia corporativa.

- **FitTrack:** FitTrack (Spix), disponible en F-Droid bajo licencia AGPL-3.0, es un rastreador fitness de código abierto desarrollado con React Native, TypeScript y arquitectura "local-first" (Zustand + MMKV). Garantiza almacenamiento exclusivo en el dispositivo, eliminando la conexión a internet y neutralizando riesgos de filtración en la nube. Prioriza la soberanía de datos: cero telemetría y sin venta de información. Funcionalmente, ofrece rutinas, gamificación y un contador de repeticiones con IA que procesa video en tiempo real sin guardar ni transmitir imágenes, incluyendo un modo alternativo solo con acelerómetro para máxima discreción. Las funciones sociales son opcionales y permite la eliminación total de datos en un clic. Esta combinación de almacenamiento local seguro, ausencia de rastreo y transparencia radical la hace ideal para activistas y usuarios que exigen independencia de ecosistemas propietarios y control absoluto sobre su información biométrica.
- **GymRoutines:** GymRoutines es una aplicación Android de código abierto (licencia GPLv3+), disponible en F-Droid y alojada en Codeberg, diseñada para crear rutinas de entrenamiento y registrar el progreso físico. Su arquitectura prioriza radicalmente la privacidad: todos los datos se almacenan exclusivamente de forma local en el dispositivo, eliminando cualquier dependencia de internet, servidores externos o sincronización en la nube que pueda comprometer la información personal. Al no requerir permisos invasivos (solo uno interno no exportado) y carecer de rastreadores o publicidad, garantiza un entorno seguro y estable. Además, al ser compilada y firmada directamente por F-Droid, se asegura la integridad del código frente a los repositorios originales, permitiendo a usuarios exigentes, activistas u organizaciones auditar su funcionamiento y confiar plenamente en que sus hábitos y datos biométricos permanecen bajo su exclusivo control, sin riesgos de filtración o mercantilización.
- **FitoTrack:** FitoTrack es un rastreador de actividad física para Android (disponible en F-Droid y Codeberg) con un enfoque radical de "privacidad

por diseño". Su arquitectura de código abierto (licencia GPLv3) opera completamente offline, eliminando cuentas, sincronización en la nube, telemetría y bases de datos remotas. Todos los datos de GPS, rendimiento y salud se almacenan exclusivamente de forma local en el dispositivo, garantizando la soberanía digital del usuario. La aplicación permite registrar y visualizar entrenamientos con mapas y estadísticas detalladas, solicitando permisos de ubicación solo en primer plano. Al carecer de anuncios y dependencias de ecosistemas propietarios, FitoTrack mitiga riesgos de explotación de datos, siendo una herramienta técnica robusta y accesible para activistas, profesionales y usuarios cotidianos que priorizan la seguridad, la independencia tecnológica y la protección integral de su información personal.

- **FitForge:** FitForge es un rastreador de fitness y nutrición en Flutter, disponible en F-Droid, que prioriza la soberanía de datos con un diseño offline-first. Toda la información (métricas, rutinas y dieta) se almacena localmente mediante `shared_preferences`, eliminando cuentas, telemetría, analíticas o rastreo de terceros. Para escenarios de riesgo, garantiza seguridad técnica robusta: el tráfico de red es exclusivamente HTTPS (forzado por `network_security_config.xml`) y cualquier clave API externa (como el coach AI opcional con Groq) se cifra mediante Android Keystore (`flutter_secure_storage`). Su naturaleza de código abierto permite auditoría completa, ofreciendo más de 110 ejercicios, planes adaptativos y seguimiento de macros sin dependencia de ecosistemas propietarios, asegurando confidencialidad, autonomía digital y protección integral de los datos personales del usuario.
- **Wger:** La aplicación Wger (Flutter) en F-Droid, cuyo código reside en github.com/wger-project/flutter, es un gestor de entrenamiento y nutrición de código abierto (AGPL-3.0+) que prioriza la soberanía de datos. Al ser autohospedable mediante Docker, permite a usuarios, activistas y organizaciones desplegar su propio backend, eliminando dependencias de ecosistemas propietarios y riesgos de vigilancia en la nube. Carece de telemetría y no comparte datos con terceros. Técnicamente, opera mediante una API REST segura, garantizando que la información sensible se almacene localmente o en servidores bajo control exclusivo del usuario. Su presencia en F-Droid asegura compilaciones reproducibles y libres de rastreadores. Esto la convierte en una herramienta robusta para escenarios de riesgo, ofreciendo cifrado en tránsito, transparencia auditable y facilidad de migración, cumpliendo con los más estrictos criterios de seguridad digital.

- **Bati**: Bati es una app para Android de código abierto (MIT) disponible en F-Droid que fusiona fitness con un RPG de fantasía oscura, donde los entrenamientos son misiones que construyen un pueblo virtual. Su arquitectura (Expo Router, SQLite con Drizzle y Zustand) garantiza soberanía digital absoluta mediante un diseño "offline-first": no realiza solicitudes de red, ni usa servidores, cuentas, analíticas o publicidad. Toda la historia de entrenamiento y datos personales se almacena exclusivamente en una base de datos local del dispositivo, eliminando riesgos de filtración en la nube o vigilancia corporativa. Al priorizar la lógica deportiva y asegurar que "nada sale de tu teléfono", Bati ofrece un modelo técnico robusto y ético que empodera al usuario con control total, privacidad intrínseca y autonomía absoluta sobre su información biométrica y de salud.
- **Martial Body:** "Martial Body" es una aplicación Android de código abierto (GPL-3.0) en F-Droid, diseñada como un programa estructurado de 24 semanas para preparar a principiantes en MMA . Técnicamente, opera 100% fuera de línea sin permisos de internet, eliminando radicalmente la telemetría, anuncios y rastreo . Utiliza Flutter, Riverpod y Drift (SQLite) para un almacenamiento local seguro, garantizando que los datos de progreso, métricas de salud y registros nunca abandonen el dispositivo . Su arquitectura prioriza la soberanía del usuario: no requiere cuentas, permite exportación CSV local y evita bibliotecas propietarias, cumpliendo rigurosamente con los estándares de F-Droid . Esto representa un modelo "privacy-by-default", donde la ausencia de llamadas a la red y la transparencia del código mitigan cualquier riesgo de fuga de datos o vigilancia digital, ofreciendo funcionalidad completa sin comprometer la seguridad personal.
- **Stepsy:** Stepsy es un contador de pasos ligero y 100% código abierto (Kotlin) para Android, disponible en F-Droid, diseñado con una arquitectura *privacy-first* que garantiza la soberanía total de los datos. Funciona completamente sin conexión a internet, eliminando cualquier riesgo de telemetría o exfiltración, ya que toda la información de actividad se procesa y almacena exclusivamente de forma local en el dispositivo. Utiliza los sensores del hardware eficientemente, ofreciendo una versión FOSS sin dependencias propietarias, mientras que su sistema avanzado de copias de seguridad automáticas protege la integridad del historial a largo plazo sin depender de la nube. Además, soporta automatización mediante *intents* personalizados (ej. Tasker), permitiendo un control granular

sobre la recolección de datos, cumpliendo rigurosamente con los más altos estándares de minimización y seguridad local para usuarios exigentes.

- **Inner Breeze:** Inner Breeze es una aplicación de código abierto (licencia MIT/BSD-3-Clause) disponible en F-Droid, diseñada para respiración, meditación y seguimiento de hábitos con un enfoque radical en la soberanía de datos. Su arquitectura "local-first" almacena toda la información en una base de datos SQLite dentro del directorio privado interno de Android (`internalDataPath`), garantizando que los datos sean inaccesibles para otras apps y se eliminen por completo al desinstalar. Carece de telemetría y solicita permisos mínimos (servicio en primer plano, evitar suspensión), eliminando riesgos de vigilancia digital, lo que la hace ideal para entornos activistas o profesionales de alto riesgo. Además, ofrece una sincronización opcional y descentralizada mediante servidores compatibles con Lyra, permitiendo a los usuarios mantener el control total de sus copias de seguridad sin depender de ecosistemas propietarios en la nube.
- **Heartwood:** Heartwood es una aplicación Android de código abierto (GPL-3.0) en F-Droid, diseñada como un visor privado y de solo lectura para Health Connect. Desarrollada con Kotlin y Jetpack Compose, visualiza métricas de salud (pasos, sueño, SpO_2, frecuencia cardíaca) mediante gráficos, resúmenes y widgets dinámicos, sin servicios externos. Su arquitectura de privacidad es estricta: carece de permisos de red, cuentas, rastreadores o telemetría, y nunca transmite datos. Funciona solicitando exclusivamente permisos de lectura local a Health Connect, otorgando al usuario control granular sobre qué datos acceder. Además, permite exportar la información a CSV/JSON localmente. Al ser una construcción reproducible y auditable, garantiza que la información sensible de salud permanezca aislada y bajo soberanía absoluta del dispositivo, eliminando riesgos de fugas, vigilancia o comercialización de datos personales.
- **Paiesque:** Paiesque es una app Android de código abierto (F-Droid, MIT) diseñada como analizador de rendimiento físico con privacidad absoluta. Funciona con arquitectura "local-first", procesando datos de sensores BLE y GPS directamente en el dispositivo, sin cuentas, minería de datos ni dependencia de nubes propietarias. Transforma la frecuencia cardíaca en métricas científicamente validadas (TRIMP, ACWR, HRV, RHR) usando fórmulas transparentes y revisadas por pares, evitando algoritmos comerciales de "caja negra". Para el trabajo colectivo, ofrece federación opcional mediante un servidor PHP autohospedado minimalista (sin base de datos), compartiendo sesiones en vivo o históricas mediante UUIDs

deterministas y claves API, garantizando que los datos grupales nunca se mezclen con los locales ni se envíen a terceros. Se integra con Health Connect, permite exportación completa a CSV/GPX y empodera al usuario con control total, soberanía digital y transparencia técnica.

- **SoloForge:** SoloForge (com.kbul.spicycrab) es un rastreador local-first de ayuno, nutrición y entrenamiento disponible en F-Droid bajo licencia GPL-3.0 . Su arquitectura en Kotlin, Jetpack Compose y Room SQLite garantiza independencia total de ecosistemas propietarios: carece de backend, autenticación, Firebase, SDKs de analítica y deshabilita el respaldo en la nube del sistema (`allowBackup=false`) . La privacidad se blinda con almacenamiento local cifrado (EncryptedSharedPreferences) y cero llamadas a red, salvo si el usuario activa voluntariamente el análisis de alimentos vía OpenRouter . Los respaldos son explícitos, versionados en JSON y fusionables, otorgando control absoluto en la migración de datos. Ideal para escenarios de riesgo (activistas, profesionales), elimina la telemetría y la dependencia de terceros, asegurando que los datos biométricos permanezcan bajo soberanía del dispositivo, sin exposición a vigilancia digital.
- **FitBook**:FitBook es una aplicación de seguimiento nutricional de código abierto y diseño *offline-first* que garantiza la soberanía de los datos al eliminar toda telemetría y dependencia de la nube. Funciona con una arquitectura local robusta en Flutter y SQLite, gestionando con precisión macros y micronutrientes, e integrando escaneo de códigos de barras opcional y gráficos de progreso avanzados. Su modo de uso se basa en permisos minimalistas y exportación nativa en formatos abiertos, otorgando al usuario control absoluto, portabilidad y privacidad total sobre su historial de salud.
- Cada una de estas apps puede configurarse, si lo permite, para exportar datos a servicios privados (por ejemplo, guardar actividad en archivos GPX o en Nextcloud), pero en esencia operan sin depender de Google Fit. Al usarlas, el usuario minimiza la fuga de datos corporativos sobre su actividad física. A nivel de resistencia, fomenta la idea de mantener los datos biométricos en entornos controlados, lejos de bases de datos globales que podrían ser usadas para manipular, segmentar o incluso discriminar.

Conclusión operacional: Para cada categoría, se recomienda configurar la aplicación alternativa como predeterminada en el sistema Android (Ajustes → Aplicaciones). Siempre que sea posible, se debe desactivar o eliminar las apps de Google correspondientes. Luego, se procede a personalizar cada alternativa:

ingresar cuentas (en cripto-servidores para correo/calendario), descargar bases (mapas en apps offline), importar datos (OPML, contactos, etc.). Los escenarios de uso incluyen: usar modos offline completo durante viajes, organizar reuniones seguras sin Play Services, o trabajar en la nube únicamente con servicios cifrados. En todos los casos, el objetivo es restablecer la soberanía tecnológica: que cada interacción (búsqueda, visualización, edición, registro, comunicación) esté bajo el control del usuario y no al servicio de un monopolio o un sistema de vigilancia centralizado.